



# Module 14: Routing Concepts

## Instructor Materials

Switching, Routing, and Wireless Essentials v7.0  
(SRWE)



# 14.1 Path Determination

## Two Functions of a Router

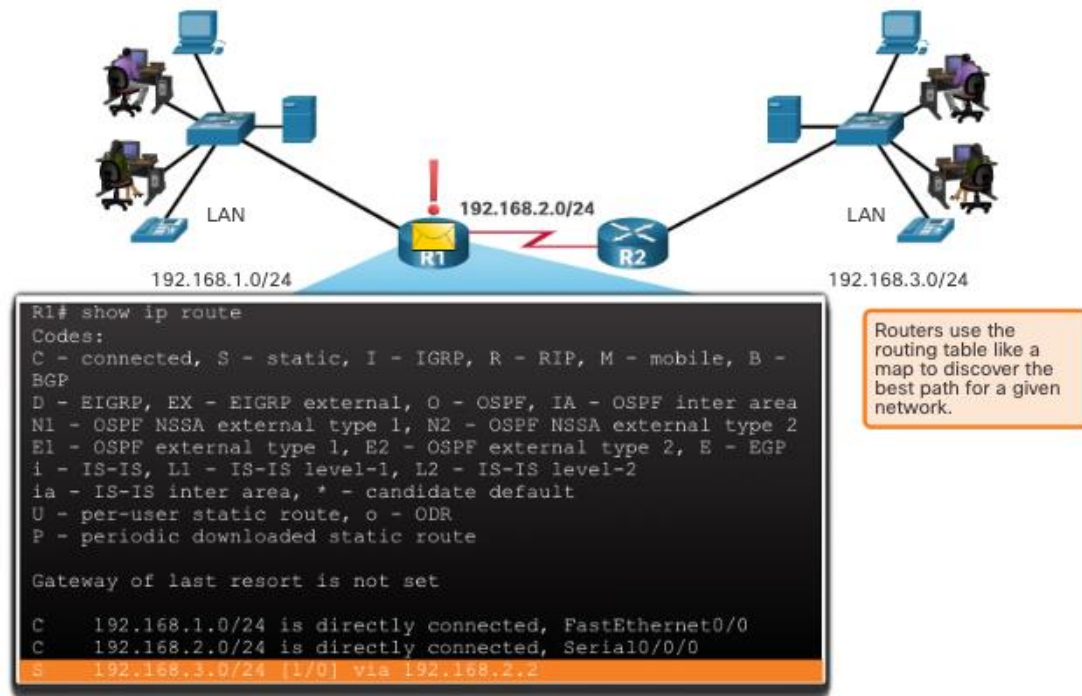
When a router receives an IP packet on one interface, it determines which interface to use to forward the packet to the destination. This is known as routing. The interface that the router uses to forward the packet may be the final destination, or it may be a network connected to another router that is used to reach the destination network. Each network that a router connects to typically requires a separate interface, but this may not always be the case.

The primary functions of a router are to determine the best path to forward packets based on the information in its routing table, and to forward packets toward their destination.

# Path Determination

## Router Functions Example

The router uses its IP routing table to determine which path (route) to use to forward a packet. R1 and R2 will use their respective IP routing tables to first determine the best path, and then forward the packet.



## Best Path Equals Longest Match

- The best path in the routing table is also known as the longest match.
- The routing table contains route entries consisting of a prefix (network address) and prefix length. For there to be a match between the destination IP address of a packet and a route in the routing table, a minimum number of far-left bits must match between the IP address of the packet and the route in the routing table. The prefix length of the route in the routing table is used to determine the minimum number of far-left bits that must match.
- The longest match is the route in the routing table that has the greatest number of far-left matching bits with the destination IP address of the packet. The longest match is always the preferred route.

**Note:** The term prefix length will be used to refer to the network portion of both IPv4 and IPv6 addresses.

## Path Determination

# IPv4 Longest Match Example

In the table, an IPv4 packet has the destination IPv4 address 172.16.0.10. The router has three route entries in its IPv4 routing table that match this packet: 172.16.0.0/12, 172.16.0.0/18, and 172.16.0.0/26. Of the three routes, 172.16.0.0/26 has the longest match and would be chosen to forward the packet. For any of these routes to be considered a match there must be at least the number of matching bits indicated by the subnet mask of the route.

| Destination IPv4 Address |                      | Address in Binary                   |
|--------------------------|----------------------|-------------------------------------|
| 172.16.0.10              |                      | 10101100.00010000.00000000.00001010 |
| Route Entry              | Prefix/Prefix Length | Address in Binary                   |
| 1                        | 172.16.0.0/12        | 10101100.00010000.00000000.00001010 |
| 2                        | 172.16.0.0/18        | 10101100.00010000.00000000.00001010 |
| 3                        | 172.16.0.0/26        | 10101100.00010000.00000000.00001010 |

# IPv6 Longest Match Example

An IPv6 packet has the destination IPv6 address 2001:db8:c000::99. This example shows three route entries, but only two of them are a valid match, with one of those being the longest match. The first two route entries have prefix lengths that have the required number of matching bits as indicated by the prefix length. The third route entry is not a match because its /64 prefix requires 64 matching bits.

| Destination |                         |                                  | 2001:db8:c000::99/48 |
|-------------|-------------------------|----------------------------------|----------------------|
| Route Entry | Prefix/Prefix Length    | Does it match?                   |                      |
| 1           | 2001:db8:c000::/40      | Match of 40 bits                 |                      |
| 2           | 2001:db8:c000::/48      | Match of 48 bits (longest match) |                      |
| 3           | 2001:db8:c000:5555::/64 | Does not match 64 bits           |                      |

## Path Determination

# Build the Routing Table

**Directly Connected Networks:** Added to the routing table when a local interface is configured with an IP address and subnet mask (prefix length) and is active (up and up).

**Remote Networks:** Networks that are not directly connected to the router. Routers learn about remote networks in two ways:

- **Static routes** - Added to the routing table when a route is manually configured.
- **Dynamic routing protocols** - Added to the routing table when routing protocols dynamically learn about the remote network.

**Default Route:** Specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. The default route can be entered manually as a static route, or learned automatically from a dynamic routing protocol.

- A default route has a /0 prefix length. This means that no bits need to match the destination IP address for this route entry to be used. If there are no routes with a match longer than 0 bits, the default route is used to forward the packet. The default route is sometimes referred to as a gateway of last resort.

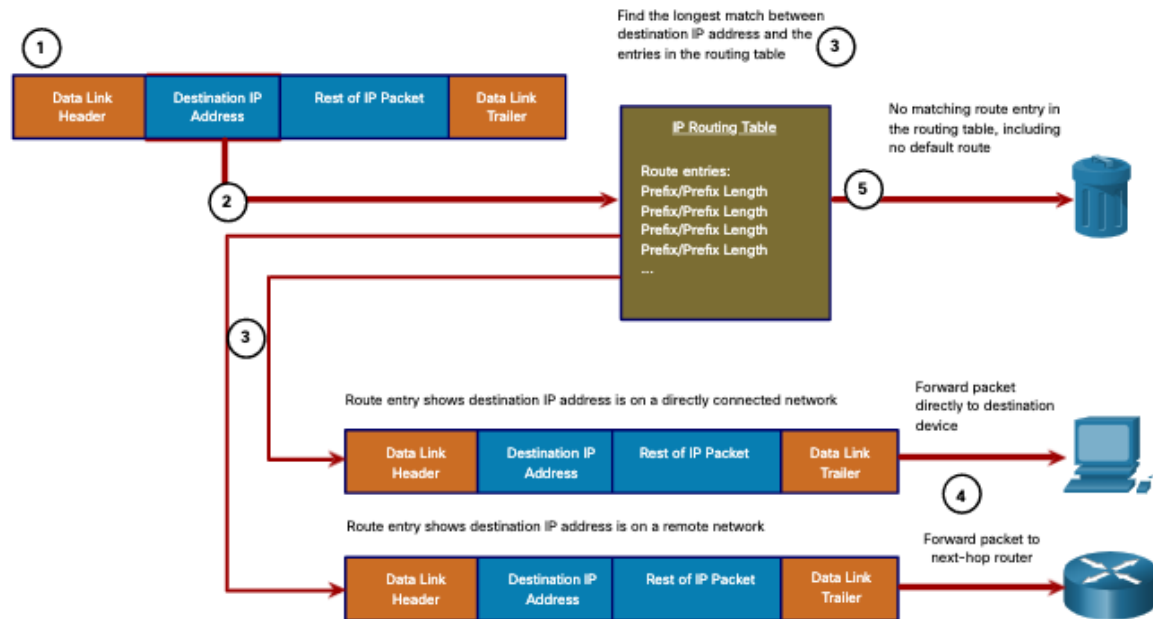


# 14.2 Packet Forwarding

# Packet Forwarding

## Packet Forwarding Decision Process

1. The data link frame with an encapsulated IP packet arrives on the ingress interface.
2. The router examines the destination IP address in the packet header and consults its IP routing table.
3. The router finds the longest matching prefix in the routing table.
4. The router encapsulates the packet in a data link frame and forwards it out the egress interface. The destination could be a device connected to the network or a next-hop router.
5. However, if there is no matching route entry the packet is dropped.



## Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

### **Forward the Packet to a Device on a Directly Connected Network**

- If the route entry indicates that the egress interface is a directly connected network, the packet can be forwarded directly to the destination device. Typically this is an Ethernet LAN.
- To encapsulate the packet in the Ethernet frame, the router needs to determine the destination MAC address associated with the destination IP address of the packet. The process varies based on whether the packet is an IPv4 or IPv6 packet.

# Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

## Forward the Packet to a Next-Hop Router

- If the route entry indicates that the destination IP address is on a remote network, meaning a device on network that is not directly connected. The packet must be forwarded to the next-hop router. The next-hop address is indicated in the route entry.
- If the forwarding router and the next-hop router are on an Ethernet network, a similar process (ARP and ICMPv6 Neighbor Discovery) will occur for determining the destination MAC address of the packet as described previously. The difference is that the router will search for the IP address of the next-hop router in its ARP table or neighbor cache, instead of the destination IP address of the packet.

**Note:** This process will vary for other types of Layer 2 networks.

## Packet Forwarding Decision Process (Cont.)

After a router has determined the best path, it could do the following:

### **Drop the Packet - No Match in Routing Table**

- If there is no match between the destination IP address and a prefix in the routing table, and if there is no default route, the packet will be dropped.

# 14.4 IP Routing Table

# IP Routing Table

## Route Sources

A routing table contains a list of routes to known networks (prefixes and prefix lengths). The source of this information is derived from the following:

- Directly connected networks
- Static routes
- Dynamic routing protocols

The source for each route in the routing table is identified by a code. Common codes include the following:

- **L** - Identifies the address assigned to a router interface.
- **C** - Identifies a directly connected network.
- **S** - Identifies a static route created to reach a specific network.
- **O** - Identifies a dynamically learned network from another router using the OSPF routing protocol.
- **\*** - This route is a candidate for a default route.

# IP Routing Table

## Routing Table Principles

There are three routing table principles as described in the table. These are issues that are addressed by the proper configuration of dynamic routing protocols or static routes on all the routers between the source and destination devices.

| Routing Table Principle  | Example  |
|--|--|
| Every router makes its decision alone, based on the information it has in its own routing table.                 | <ul style="list-style-type: none"><li>•R1 can only forward packets using its own routing table.</li><li>•R1 does not know what routes are in the routing tables of other routers (e.g., R2).</li></ul>   |
| The information in a routing table of one router does not necessarily match the routing table of another router. | Just because R1 has route in its routing table to a network in the internet via R2, that does not mean that R2 knows about that same network.  |
| Routing information about a path does not provide return routing information.                                    | R1 receives a packet with the destination IP address of PC1 and the source IP address of PC3. Just because R1 knows to forward the packet out its G0/0/0 interface, doesn't necessarily mean that it knows how to forward packets originating from PC1 back to the remote network of PC3 |



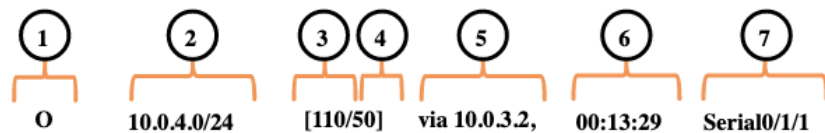
# IP Routing Table

## Routing Table Entries

In the figure, the numbers identify the following information:

- **Route source** - This identifies how the route was learned.
- **Destination network (prefix and prefix length)** - This identifies the address of the remote network.
- **Administrative distance** - This identifies the trustworthiness of the route source. Lower values indicate preferred route source.
- **Metric** - This identifies the value assigned to reach the remote network. Lower values indicate preferred routes.
- **Next-hop** - This identifies the IP address of the next router to which the packet would be forwarded.
- **Route timestamp** - This identifies how much time has passed since the route was learned.
- **Exit interface** - This identifies the egress interface to use for outgoing packets to reach their final destination.

IPv4 Routing Table



IPv6 Routing Table



**Note:** The prefix length of the destination network specifies the minimum number of far-left bits that must match between the IP address of the packet and the destination network (prefix) for this route to be used.

## IP Routing Table

# Directly Connected Networks

To learn about any remote networks, the router must have at least one active interface configured with an IP address and subnet mask (prefix length). This is known as a directly connected network or a directly connected route. Routers add a directly connected route to its routing table when an interface is configured with an IP address and is activated.

- A directly connected network is denoted by a status code of **C** in the routing table. The route contains a network prefix and prefix length.
- The routing table also contains a local route for each of its directly connected networks, indicated by the status code of **L**.
- For IPv4 local routes the prefix length is /32 and for IPv6 local routes the prefix length is /128. This means the destination IP address of the packet must match all the bits in the local route for this route to be a match. The purpose of the local route is to efficiently determine when it receives a packet for the interface instead of a packet that needs to be forwarded.

# IP Routing Table

## Static Routes

After directly connected interfaces are configured and added to the routing table, static or dynamic routing can be implemented for accessing remote networks. Static routes are manually configured. They define an explicit path between two networking devices. They are not automatically updated and must be manually reconfigured if the network topology changes.

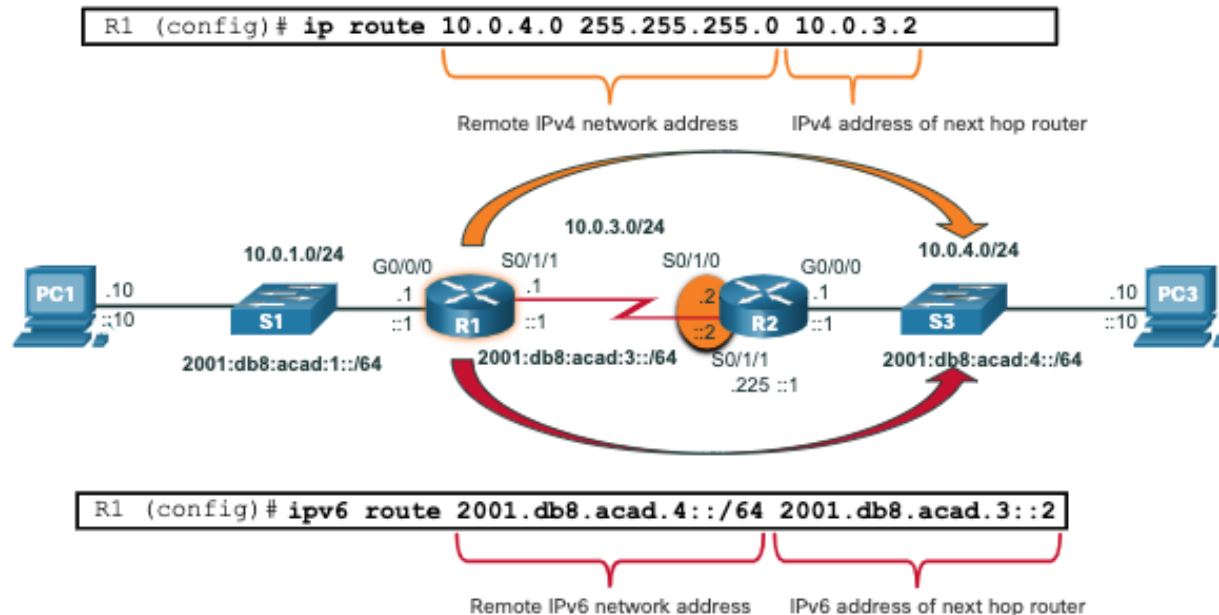
Static routing has three primary uses:

- It provides ease of routing table maintenance in smaller networks that are not expected to grow significantly.
- It uses a single default route to represent a path to any network that does not have a more specific match with another route in the routing table. Default routes are used to send traffic to any destination beyond the next upstream router.
- It routes to and from stub networks. A stub network is a network accessed by a single route, and the router has only one neighbor.

# IP Routing Table

## Static Routes in the IP Routing Table

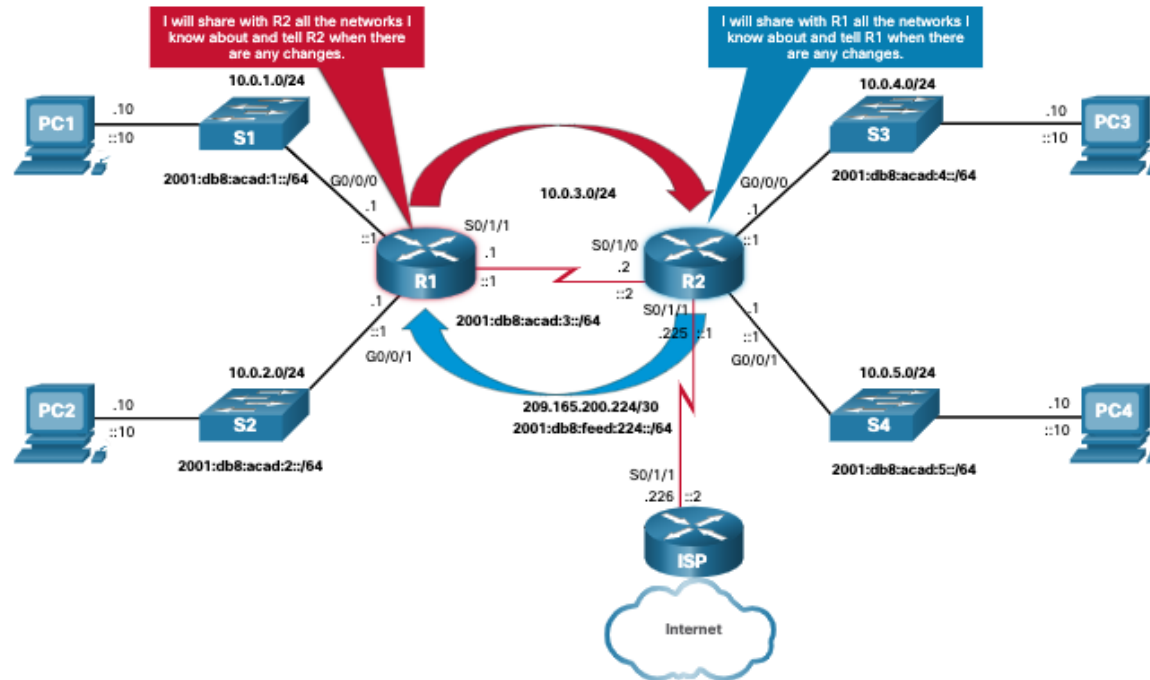
The topology in the figure is simplified to show only one LAN attached to each router. The figure shows IPv4 and IPv6 static routes configured on R1 to reach the 10.0.4.0/24 and 2001:db8:acad:4::/64 networks on R2.



# IP Routing Table

## Dynamic Routing Protocols

Dynamic routing protocols are used by routers to automatically share information about the reachability and status of remote networks. Dynamic routing protocols perform several activities, including network discovery and maintaining routing tables.



# IP Routing Table

## Dynamic Routes in the Routing Table

OSPF is now being used in our sample topology to dynamically learn all the networks connected to R1 and R2. The routing table entries use the status code of **O** to indicate the route was learned by the OSPF routing protocol. Both entries also include the IP address of the next-hop router, via *ip-address*.

**Note:** IPv6 routing protocols use the link-local address of the next-hop router.

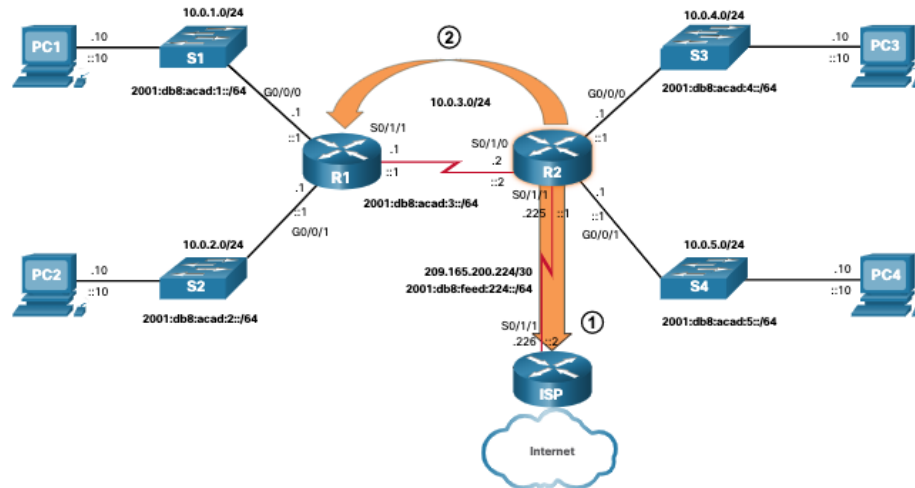
**Note:** OSPF routing configuration for IPv4 and IPv6 is beyond the scope of this course.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP,
EX - EIGRP external, O - OSPF, IA - OSPF inter area
(output omitted for brevity)
O 10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O 10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
NDR - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O 2001:DB8:ACAD:4::/64 [110/50]
  via FE80::2:C, Serial0/1/1
O 2001:DB8:ACAD:5::/64 [110/50]
  via FE80::2:C, Serial0/1/1
```

# IP Routing Table

## Default Route

The default route specifies a next-hop router to use when the routing table does not contain a specific route that matches the destination IP address. A default route can be either a static route or learned automatically from a dynamic routing protocol. A default route has an IPv4 route entry of 0.0.0.0/0 or an IPv6 route entry of ::/0. This means that zero or no bits need to match between the destination IP address and the default route.



## IP Routing Table

# Administrative Distance

A route entry for a specific network address (prefix and prefix length) can only appear once in the routing table. However, it is possible that the routing table learns about the same network address from more than one routing source. Except for very specific circumstances, only one dynamic routing protocol should be implemented on a router. Each routing protocol may decide on a different path to reach the destination based on the metric of that routing protocol.

This raises a few questions, such as the following:

- How does the router know which source to use?
- Which route should it install in the routing table?

Cisco IOS uses what is known as the administrative distance (AD) to determine the route to install into the IP routing table. The AD represents the "trustworthiness" of the route. The lower the AD, the more trustworthy the route source.



# IP Routing Table

## Administrative Distance (Cont.)

The table lists various routing protocols and their associated ADs.

| Route Source        | Administrative Distance |
|---------------------|-------------------------|
| Directly connected  | 0                       |
| Static route        | 1                       |
| EIGRP summary route | 5                       |
| External BGP        | 20                      |
| Internal EIGRP      | 90                      |
| OSPF                | 110                     |
| IS-IS               | 115                     |
| RIP                 | 120                     |
| External EIGRP      | 170                     |
| Internal BGP        | 200                     |

# 14.5 Static and Dynamic Routing

# Static and Dynamic Routing

## Static or Dynamic? (Cont.)

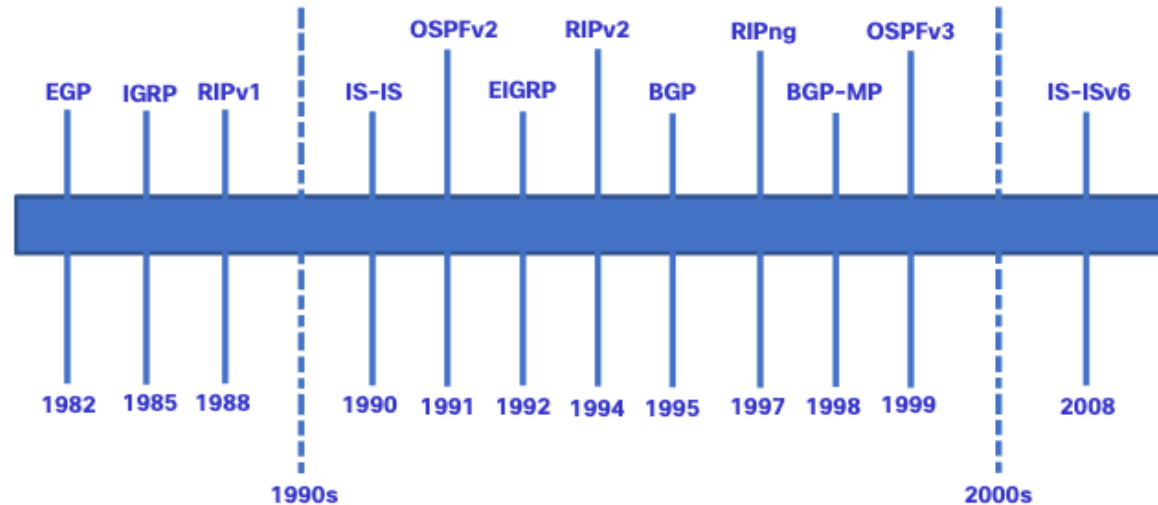
The table shows a comparison of some the differences between dynamic and static routing.

| Feature                  | Dynamic Routing                                     | Static Routing                          |
|--------------------------|---|---|
| Configuration complexity | Independent of network size                         | Increases with network size             |
| Topology changes         | Automatically adapts to topology changes            | Administrator intervention required     |
| Scalability              | Suitable for simple to complex network topologies   | Suitable for simple topologies          |
| Security                 | Security must be configured                         | Security is inherent                    |
| Resource Usage           | Uses CPU, memory, and link bandwidth                | No additional resources needed          |
| Path Predictability      | Route depends on topology and routing protocol used | Explicitly defined by the administrator |

# Static and Dynamic Routing

## Dynamic Routing Evolution

Dynamic routing protocols have been used in networks since the late 1980s. One of the first routing protocols was RIP. RIPv1 was released in 1988, but some of the basic algorithms within the protocol were used on the Advanced Research Projects Agency Network (ARPANET) as early as 1969. As networks evolved and became more complex, new routing protocols emerged.



# Static and Dynamic Routing

## Dynamic Routing Evolution (Cont.)

The table classifies the current routing protocols. Interior Gateway Protocols (IGPs) are routing protocols used to exchange routing information within a routing domain administered by a single organization. There is only one EGP and it is BGP. BGP is used to exchange routing information between different organizations, known as autonomous systems (AS). BGP is used by ISPs to route packets over the internet. Distance vector, link-state, and path vector routing protocols refer to the type of routing algorithm used to determine best path.

|      | Interior Gateway Protocols |                |            |                | Exterior Gateway Protocols |
|------|----------------------------|----------------|------------|----------------|----------------------------|
|      | Distance Vector            |                | Link-State |                | Path Vector                |
| IPv4 | RIPv2                      | EIGRP          | OSPFv2     | IS-IS          | BGP-4                      |
| IPv6 | RIPng                      | EIGRP for IPv6 | OSPFv3     | IS-IS for IPv6 | BGP-MP                     |

## Static and Dynamic Routing

# Dynamic Routing Protocol Concepts

A routing protocol is a set of processes, algorithms, and messages that are used to exchange routing information and populate the routing table with the choice of best paths. The purpose of dynamic routing protocols includes the following:

- Discovery of remote networks
- Maintaining up-to-date routing information
- Choosing the best path to destination networks
- Ability to find a new best path if the current path is no longer available

## Dynamic Routing Protocol Concepts (Cont.)

The main components of dynamic routing protocols include the following:

- **Data structures** - Routing protocols typically use tables or databases for their operations. This information is kept in RAM.
- **Routing protocol messages** - Routing protocols use various types of messages to discover neighboring routers, exchange routing information, and other tasks to learn and maintain accurate information about the network.
- **Algorithm** - An algorithm is a finite list of steps used to accomplish a task. Routing protocols use algorithms for facilitating routing information and for the best path determination.

Routing protocols determine the best path, or route, to each network. That route is then offered to the routing table. The route will be installed in the routing table if there is not another routing source with a lower AD.

# Static and Dynamic Routing

## Best Path

The best path is selected by a routing protocol based on the value or metric it uses to determine the distance to reach a network. A metric is the quantitative value used to measure the distance to a given network. The best path to a network is the path with the lowest metric.

Dynamic routing protocols typically use their own rules and metrics to build and update routing tables. The following table lists common dynamic protocols and their metrics.

| Routing Protocol  | Metric  |
|---|---|
| <b>Routing Information Protocol (RIP)</b>                 | <ul style="list-style-type: none"><li>•The metric is “hop count”.</li><li>•Each router along a path adds a hop to the hop count.</li><li>•A maximum of 15 hops allowed.</li></ul>   |
| <b>Open Shortest Path First (OSPF)</b>                    | <ul style="list-style-type: none"><li>•The metric is “cost” which is based on the cumulative bandwidth from source to destination.</li><li>•Faster links are assigned lower costs compared to slower (higher cost) links.</li></ul> |
| <b>Enhanced Interior Gateway Routing Protocol (EIGRP)</b> | <ul style="list-style-type: none"><li>•It calculates a metric based on the slowest bandwidth and delay values.</li><li>•It could also include load and reliability into the metric calculation.</li></ul>                           |



## Static and Dynamic Routing

# Load Balancing

When a router has two or more paths to a destination with equal cost metrics, then the router forwards the packets using both paths equally. This is called equal cost load balancing.

- The routing table contains the single destination network, but has multiple exit interfaces, one for each equal cost path. The router forwards packets using the multiple exit interfaces listed in the routing table.
- If configured correctly, load balancing can increase the effectiveness and performance of the network.
- Equal cost load balancing is implemented automatically by dynamic routing protocols. It is enabled with static routes when there are multiple static routes to the same destination network using different next-hop routers.

**Note:** Only EIGRP supports unequal cost load balancing.

# 14.6 Module Practice and Quiz